CLAIMS

What is claimed is:

1. A method of producing a uniform duty cycle output from a random bit source, the method comprising:

testing the duty cycle of the random bit source;

varying the output voltage of a voltage source if the duty cycle is not substantially fifty percent; and

iteratively altering the output voltage of the voltage source until the duty cycle is substantially fifty percent.

2. The method of claim 1 further comprising:

periodically latching a high frequency signal in response to a low frequency signal; and

outputting one or more binary digits corresponding to a voltage level of the latching high frequency signal.

3. The method of claim 1 wherein varying the output voltage of the voltage circuit further comprises updating the threshold voltage of a flash memory cell in the voltage circuit.

4. The method of claim 1 wherein varying the output voltage of the voltage circuit further comprises:

varying an input current to a non-inverting input of a differential amplifier to produce a first input voltage; and

varying an input current to an inverting input of the differential amplifier to produce a second input voltage.

5. The method of claim 1 wherein varying the output voltage of the voltage circuit further comprises altering the number of transistors in the voltage circuit determining the output voltage.

6. The method of claim 1 wherein the method of producing a uniform duty cycle output from a random bit source is used in a random number generator operable to produce random binary numbers for use in a cryptographic system for secure communications between a plurality of computers in a network.

7. A programmable random bit source comprising:

a latch having a data input and a clock input;

a first oscillator coupled to the data input of the latch, the first oscillator to output a first oscillating signal; and

a second oscillator coupled to the clock input of the latch circuit, the second oscillator to output a second oscillating signal having a frequency slower than a frequency of the first oscillating signal.

8. The programmable random bit source of claim 7 further comprising a programmable voltage source coupled to a bias input of the latch.

9. The programmable random bit source of claim 8 wherein the programmable voltage source comprises:

a first flash memory cell;

a second flash memory cell; and

a differential amplifier having a first input coupled to the first flash memory cell, and a second input coupled to the second flash memory cell.

10. The programmable random bit source of claim 7 wherein the programmable voltage source comprises:

a first resistor;

a second resistor; and

a differential amplifier having a first input coupled to the first resistor, and a second input coupled to the second resistor.

11. The programmable random bit source of claim 7 wherein the programmable voltage source comprises a logic gate having:

a first pull-up transistor;

a first pull-down transistor; and

a second pull-up transistor coupled in parallel with the first pull-up transistor.

12. The programmable random bit source of claim 11 wherein the logic gate further comprises means for selectively enabling the second pull-up transistor.

13. The programmable random bit source of claim 7 wherein the programmable voltage source comprises a logic gate having:

a first pull-up transistor;

a first pull-down transistor; and

a second pull-down transistor coupled in parallel with the first pull-down transistor.

14. The programmable random bit source of claim 13 wherein the logic gate further comprises means for selectively enabling the second pull-down transistor.

15. The programmable random bit source of claim 7 wherein the latch has an adjustable trip point.

16. The programmable random bit source of claim 15 further comprising a programmable voltage source coupled to a bias input of the latch, wherein the adjustable trip point of the latch is alterable by a voltage output by the programmable voltage source.

17. A programmable random bit source comprising:

a latch having a data input and a bias input;

a programmable voltage source coupled to the bias input of the latch;

a comparator having an output coupled to the data input of the latch;

a resistor-inductor-capacitor circuit coupled to an input of the comparator; and

a noise source coupled to the resistor-inductor-capacitor circuit.

18. The programmable random bit source of claim 17 wherein the latch has an alterable trip point.

19. A digital processing system comprising:

an encryption/decryption circuit comprising a random number generator having,

a latch having a data input and a clock input;

a first oscillator coupled to the data input of the latch, the first oscillator to output a first oscillating signal; and

a second oscillator coupled to the clock input of the latch circuit, the second oscillator to output a second oscillating signal having a frequency slower than a frequency of the first oscillating signal.

20. The digital processing system of claim 19 wherein the programmable bit source further includes a programmable voltage source coupled to a bias input of the latch.

21. The digital processing system of claim 20 wherein the latch has an adjustable trip point, wherein the adjustable trip point of the latch is alterable by a voltage output by the programmable voltage source.

22. The digital processing system of claim 19 wherein the encryption/decryption circuit to encode and decode messages transmitted and received by the digital processing system using a cipher-based cryptographic method.

23. The digital processing system of claim 22 wherein the cipher-based cryptographic method is a single key system.

24. The digital processing system of claim 22 wherein the cipher-based cryptographic method is a public key/private key system.